UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/936,157	09/06/2001	Osamu Shibata	NAKI-BP89	9192

7590 08/13/2003

Joseph W Price
Price & Gess
Suite 250
2100 SE Main Street
Irvine, CA 92614

EXAMINER
MOORTHY, ARAVIND K

ART UNIT	PAPER NUMBER
2131	7

DATE MAILED: 08/13/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/936,157	SHIBATA ET AL.	
	Examiner	Art Unit	
	Aravind K Moorthy	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 July 2002* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-16* is/are rejected.

7)☒ Claim(s) *13-16* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *06 September 2001* is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) *3, 6* .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Claim Objections

1. **Claims 13-16 are objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim.**

Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form.

Claim 13 recites the limitation "an access device which is included in the authentication communication system" is already claimed in claim 1 and does not further limit claim 1.

Claim 14 recites the limitation "an access device which is included in the authentication communication system" is already claimed in claim 2 and does not further limit claim 2.

Claim 15 recites the limitation "a storage medium which is included in the authentication communication system" is already claimed in claim 1 and does not further limit claim1.

Claim 16 recites the limitation "a storage medium which is included in the authentication communication system" is already claimed in claim 3 and does not further limit claim 3.

A series of singular dependent claims is permissible in which a dependent claim refers to a preceding claim which, in turn, refers to another preceding claim.

2. **A claim that depends from a dependent claim should not be separated by any claim that does not also depend from said dependent claim.**

Claim 13 is depends on claim 1. Claim 14 depends on claim 2. Claim 15 depends on claim 1. Claim 16 depends on claim 3. It should be kept in mind that a dependent claim may refer to any preceding independent claim. In general, applicant's sequence will not be changed. See MPEP § 608.01(n).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-3 and 8-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Zuk U.S. Patent No. 5,745,571 in view of Antognini et al U.S. Patent No. 5,649,185.

As to claim 1, 11 and 12, Zuk discloses a first authentication phase in which the access device authenticates whether the storage medium is authorized according to a challenge-response authentication protocol [column 5, lines 1-26]. Zuk discloses a second authentication phase in which the storage medium authenticates whether the access device is authorized [column 5 line 65 to column 6 line 2]. Zuk discloses a transfer phase in which, when the storage medium and the access device have authenticated each other as authorized devices [column 5, lines 37-48]. Zuk discloses that the access device reads/writes digital information from/into the second device [column 5, lines 37-48]. Zuk teaches transmitting scrambled information [abstract].

Zuk does not teach that the first authentication phase includes transmitting scrambled access information generated by scrambling access information that shows the area, to the storage medium. Zuk does not teach the storage medium extracts the access information from the scrambled access information.

Antognini et al teaches an authentication that includes transmitting access information that shows the area to the storage medium [column 9, lines 33-43]. Antognini et al teaches that the storage medium extracts the access information [column 9, lines 60-65].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Zuk so that the first authentication phase would have included scrambled access information that showed area on the storage medium. The identifier would have been combined with the random number. The combination would have been then scrambled. The storage medium would have extracted the access information from the scrambled access information.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Zuk by the teaching of Antognini et al because this technique will provide image identifiers that are unique within any library and which are never reused [column 22, lines 22-24].

As to claim 2, the Zuk-Antognini combination teaches that in the first authentication phase, the access device includes: an access information acquisition unit for acquiring the access information which shows the area, as discussed above; a random number acquisition unit for acquiring a random number [Zuk column 4, lines 12-23]; a generation unit for generating random number access information by combining the access information and the random number, as discussed above; and an encryption unit for encrypting the random number access information according to an encryption algorithm to generate the scrambled access information [Zuk column 4, lines 16-20]. The Zuk-Antognini combination teaches that the storage medium includes a response value generation unit for generating a response value from the scrambled

access information [Zuk column 5, lines 1-26]. The Zuk-Antognini combination teaches that the access device includes an authentication unit for authenticating whether the storage medium is authorized using the response value [Zuk column 5, lines 1-26].

As to claim 3, the Zuk-Antognini combination teaches that in the transfer phase, the storage medium includes: a decryption unit for decrypting the scrambled access information according to a decryption algorithm to obtain the random number access information [Zuk column 4, lines 24-43]; and a separation unit for separating the access information from the random number access information, as discussed above.

As to claim 8, the Zuk-Antognini combination teaches that the storage medium, which stores digital information in the area, includes an encryption unit for reading the digital information from the area shown by the access information and encrypting the digital information according to an encryption algorithm to generate encrypted digital information [Zuk column 3, lines 53-67]. The Zuk-Antognini combination teaches that the access device, which reads the digital information from the area, includes a decryption unit for decrypting the encrypted digital information according to a decryption algorithm to obtain the digital information, as discussed above, the decryption algorithm being an algorithm for decrypting a cryptogram generated according to the encryption algorithm, as discussed above.

As to claim 9, the Zuk-Antognini combination teaches that in the transfer phase, the access device, which writes digital information into the area, includes: a digital information acquisition unit for acquiring the digital information [i.e. smart card]; and an encryption unit for encrypting the digital information according to an encryption algorithm to generate encrypted digital information, as discussed above. The Zuk-Antognini combination teaches that the storage

medium includes a decryption unit for decrypting the encrypted digital information according to a decryption algorithm to obtain the digital information, and writing the digital information into the area shown by the access information, as discussed above. The Zuk-Antognini combination teaches that the decryption algorithm being an algorithm for decrypting a cryptogram generated according to the encryption algorithm [Zuk column 3, lines 53-67].

As to claim 13, the Zuk-Antognini combination teaches an access device that is included in the authentication communication [Zuk column 3, lines 18-35].

As to claim 14, the Zuk-Antognini combination teaches an access device that is included in the authentication communication [Zuk column 3, lines 18-35].

As to claim 15, the Zuk-Antognini combination teaches a storage medium that is included in the authentication communication [Zuk column 3, lines 18-35].

As to claim 16, the Zuk-Antognini combination teaches a storage medium which is included in the authentication communication system [Zuk column 3, lines 18-35].

4. Claims 4-7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Zuk U.S. Patent No. 5,745,571 and Antognini et al U.S. Patent No. 5,649,185 as applied to claim 1 above, and further in view of Vobach U.S. Patent No. 5,193,115.

As to claim 4, the Zuk-Antognini combination does not teach that in the first authentication phase, the access device further includes a random number seed storage unit for storing a random number seed, and the random number acquisition unit acquires the random number by reading the random number seed from the random number seed storage unit.

Vobach teaches a random number seed storage unit for storing a random number seed, and the random number acquisition unit acquires the random number by reading the random number seed from the random number seed storage unit [column 9, lines 21-39].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Zuk-Antognini combination so that the random number are created with a random number seed that is stored in a storage unit. The random numbers would have been acquired from the storage unit.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Zuk-Antognini combination by the teaching of Vobach because the masking tape string only appears to an eavesdropper as a summand of the known ciphertext string, reconstructing it depends upon knowing the plaintext message string. Since, for a given encrypted message, there will be many equally probably possible plaintext message strings, there will be as many equally probable possible masking tape strings. In short, the plaintext message string "masks" the masking tape string [column 6 line 64 to column 7 line 8].

As to claim 5, the Zuk-Antognini-Vobach combination teaches that in the first authentication phase, the access device further writes the scrambled access information over the random number seed stored in the random number seed storage unit, as a new random number seed [Vobach column 9, lines 40-63].

As to claim 6, the Zuk-Antognini-Vobach combination teaches that in the first authentication phase, the access device further includes a random number seed storage unit for storing a random number seed, and the random number acquisition unit acquires the random number, by reading the random number seed from the random number seed storage unit and

generating the random number based on the random number seed [Vobach column 9, lines 21-63].

As to claim 7, the Zuk-Antognini-Vobach combination teaches that in the first authentication phase, the access device further writes the random number over the random number seed stored in the random number seed storage unit as a new random number seed, as discussed above.

5. Claims 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over Zuk U.S. Patent No. 5,745,571 and Antognini et al U.S. Patent No. 5,649,185 as applied to claim 1 above, and further in view of Appelbaum et al U.S. Patent No. 4,683,968.

As to claim 10, the Zuk-Antognini combination teaches a digital information acquisition unit for acquiring the digital information, as discussed above; a content key acquisition unit for acquiring a content key [Zuk column 5, lines 1-26]; a first encryption unit for encrypting the acquired content key according to a first encryption algorithm to generate an encrypted content key [Zuk column 5, lines 1-26]; and the storage medium further includes an area for storing the encrypted digital information [Zuk figure 1]. The Zuk-Antognini combination teaches generating encrypted digital information,

The Zuk-Antognini combination does not teach a second encryption unit for encrypting the encrypted content key according to a second encryption algorithm to generate a double-encrypted content key; and a third encryption unit for encrypting the digital information according to a second encryption algorithm using the content key. The Zuk-Antognini does not teach that the storage medium includes a decryption unit for decrypting the double-encrypted

content key according to a first decryption algorithm to obtain the encrypted content key, and writing the encrypted content key into the area shown by the access information.

Appelbaum et al teaches an encryption unit for encrypting the encrypted key according to a second encryption algorithm to generate a double-encrypted key [figure 1]; and a third encryption unit for encrypting the digital information according to a second encryption algorithm using a key [figure 2]. Appelbaum et al teaches a decryption unit for decrypting the double-encrypted content key according to a first decryption algorithm to obtain the encrypted content key, and writing the encrypted content key into the area shown by the access information [figures 1 and 3].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Zuk-Antognini combination so that content key as taught by Zuk would have been double encrypted using a second encryption algorithm as taught by Appelbaum et al. There would have been a decryption unit using the same decryption algorithm to decrypt the encrypted content key and written to the storage area shown by the identifier.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Zuk-Antognini combination by the teaching of Appelbaum et al because the examiner asserts that a double encrypted key provides enhanced security.

Conclusion

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K Moorthy whose telephone number is 703-305-1373. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 703-305-9648. The fax phone numbers for the organization where this application or proceeding is assigned are 703-746-7239 for regular communications and 703-746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-1373.

Aravind K. Moorthy
August 7, 2003

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100